Il nuovo anno è iniziato con la preoccupante notizia (almeno da un punto di vista informatico) dell'esistenza di due nuove vulnerabilità presenti praticamente in tutti i computer recenti, ma anche in smartphone e tablet, denominate "Meltdown" e "Spectre". Cerchiamo di seguito di fare un po' di chiarezza sull'argomento.
Per chi volesse approfondire ulteriormente l'argomento, ecco un utile link: https://meltdownattack.com/.

**MELTDOWN**

La vulnerabilità denominata Meltdown è stata scoperta e riportata in modo indipendente da tre gruppi di ricercatori: Jann Horn (Google Project Zero), Werner Haas, Thomas Prescher (Cyberus Technology), Daniel Gruss, Moritz Lipp, Stefan Mangard, Michael Schwarz (Graz University of Technology).
Il nome deriva dal fatto che la vulnerabilità "fonde" per così dire la separazione logica che i moderni microprocessori creano tra lo spazio di memoria RAM utilizzato dai programmi ordinari e quello riservato al sistema operativo che fa lavorare il computer (Windows, Apple OS-X e Linux). Normalmente un programma in esecuzione non può accedere ad aree di memoria esterne a quelle che il sistema operativo gli assegna per depositare i suoi dati: se si tenta di leggere i dati da un'altra area di memoria il processore genera un errore ed il sistema blocca il programma.
La vulnerabilità Meltdown è legata all'architettura interna dei microprocessori: quando un programma viene eseguito il suo codice macchina è suddiviso tra tutte le unità di esecuzione delle singole istruzioni che prelevano i dati da piccole memorie ad altissima velocità, dette memorie cache di livello 1, 2 e 3. Se il dato desiderato non si trova in quel momento nella cache viene richiesto alla memoria RAM: il tempo necessario ad ottenere il dato è piccolo ma molto lungo rispetto alla velocità a cui lavora il processore, che dovrebbe restare in attesa perdendo tempo prezioso. Per non sprecare questo tempo è stata quindi introdotta la funzionalità detta "out of order execution".
Se un'unità di esecuzione è ferma in attesa di un dato, un'altra continua a lavorare sulle istruzioni successive del programma: se l'attaccante richiede la lettura da un'area di memoria protetta mentre il dato viene caricato le altre istruzioni successive verranno comunque eseguite. Quando la prima unità di esecuzione si accorge dell'errore (accesso ad area protetta) il processore segnala la violazione ed il programma viene arrestato, tuttavia è possibile far sì che una piccola parte di altri dati protetti siano stati nel frattempo caricati nella memoria cache e trasferiti in un'area di memoria del programma malevolo grazie alle operazioni svolte "out of order" dalla seconda unità di esecuzione.
Con un uso sofisticato del codice macchina è stato dimostrato che è possibile copiare dentro alla memoria assegnata ad un programma tutto il contenuto della memoria del computer, comprese le aree riservate del sistema operativo ed i suoi dati normalmente nascosti, rendendo visibili anche dati protetti.
Qui a fianco il frammento di programma eletto a simbolo della vulnerabilità Meltdown.

```
meltdown:
mov al, byte [rcx]
shl rax, 0xc
jz meltdown
mov rbx, qword [rbx + rax]
```

La vulnerabilità Meltdown è presente in tutti i processori Intel prodotti dopo il 1995 (salvo poche eccezioni): non è chiaro se riguardi anche i processori AMD ed è comunque presente in alcuni modelli di processori ARM (che equipaggiano smartphone e tablet). I produttori di microprocessori e di sistemi operativi sono stati di recente avvisati del problema e sono in corso i lavori per ridurre i rischi di questa vulnerabilità. In particolare sono già state rilasciate correzioni per i sistemi Windows, Linux e OS-X, anche se per eliminare definitivamente il problema sarà necessario intervenire sulla progettazione hardware dei futuri processori poiché la semplice eliminazione delle elaborazioni "out of order" provocherebbe un inaccettabile calo di prestazioni di tutti i dispositivi.
Non sono ancora noti attacchi Meltdown effettuati su computer operativi, tuttavia un simile tipo di attacco sarebbe difficile da rivelare perché quasi indistinguibile dalle operazioni svolte da un programma ordinario. C'è da dire che per eseguire un attacco Meltdown il computer deve essere infettato dal programma sabotatore, quindi un buon antivirus aggiornato resta un elemento fondamentale di protezione.

**SPECTRE**

La vulnerabilità Spectre è stata scoperta e segnalata in modo indipendente da due gruppi di lavoro: Jann Horn (Google Project Zero) e Paul Kocher (in collaborazione con Daniel Genkin, Mike Hamburg, Moritz Lipp, e Yuval Yarom.
Il nome Spectre è suggerito dall'uso della cosiddetta "esecuzione speculativa" e dal fatto che - poiché è di difficile correzione - questa vulnerabilità si aggirerà per parecchio tempo tra i nostri computer, proprio come se fosse un fantasma…
Spectre è una vulnerabilità universale in quanto sfrutta la cosiddetta "esecuzione speculativa" presente su tutti i processori moderni. Questa tecnica consiste nell'eseguire in anticipo delle istruzioni di un programma che sono soggette ad una condizione iniziale durante il tempo necessario a valutare se la condizione è vera, nell'ipotesi che lo sia effettivamente e quindi si possa guadagnare tempo prezioso nell'elaborazione dei risultati.
L'esecuzione speculativa avviene sulla base del fatto che nelle valutazioni precedenti la condizione è sempre stata vera e quindi è probabile che lo sia ancora: se invece la condizione si rivela falsa il codice macchina che non dovrebbe essere eseguito in realtà è già stato eseguito da un'altra unità di elaborazione del processore (in modo analogo a quanto descritto per la vulnerabilità Meltdown) ed è possibile che alcuni dati che non dovrebbero essere letti dalla memoria RAM del programma siano in realtà già stati caricati nella memoria cache, da cui possono rapidamente essere trasferiti all'attaccante.
Con una attenta scelta delle istruzioni speculative eseguite si è dimostrato possibile copiare aree della memoria di un programma in esecuzione normalmente invisibili al programma spia e mostrare in chiaro dati riservati e password.
La tecnica utilizzata da Spectre è ben simboleggiata dal frammento di codice riportato sotto.

```
if (x < array1_size)
    y = array2[array1[x] * 256];
```

Come Meltdown, anche Spectre sfrutta il modo di funzionamento di un microprocessore ma a differenza del caso precedente lo usa per "trarre in inganno" un programma normale in esecuzione sul computer ed accedere ad aree riservate della sua memoria di lavoro. L'uso della vulnerabilità richiede uno studio attento dei programmi bersaglio ma in compenso può essere anche realizzato con delle istruzioni in linguaggio Javascript (normalmente usate in tutti i siti web) per accedere alla memoria di un comune browser Internet e rivelare nomi utente e password.
Spectre è una vulnerabilità di difficile risoluzione, anche se è più complesso allestire un programma malevolo che la sfrutti. Come nel caso precedente non sono ancora noti attacchi Spectre effettuati su computer operativi anche se la rilevazione dell'attacco sarebbe comunque difficile.
Come già per Meltdown, anche per Spectre l'attivazione della vulnerabilità è difficile da rivelare perché quasi indistinguibile dalle operazioni svolte da un programma ordinario; anche in questo caso però il computer deve comunque essere infettato dal programma sabotatore, quindi antivirus e aggiornamenti del sistema operativo restano fondamentali per minimizzare i rischi.